Ma, W., Liu, W., Luo, X., McAreavey, K., Jiang, Y., & Ma, J. (2019). A Dempster-Shafer theory and uninorm-based framework of reasoning and multiattribute decision-making for surveillance system. *International Journal of Intelligent Systems*, *34*(11), 3077-3104. https://doi.org/10.1002/int.22175

A D-S Theory and Uninorm Based Framework of Reasoning and Multi-Attribute Decision Making for Surveillance System

Wenjun Ma[1], Weiru Liu[2], Xudong Luo[3‡], Kevin McAreavey[2], Yuncheng Jiang[1¶], and Jianbing Ma[4]

[1] *School of Computer Science, South China Normal University, Guangzhou, China.*
[2] *School of Computer Science, Electrical and Electronic Engineering, and Engineering Maths, University of Bristol, Bristol, UK.*
[3] *Department of Information and Management Science, Guangxi Normal University, Guilin, China.*
[4] *School of Computing, Electronics and Mathematics, Coventry University, UK*

ABSTRACT

CCTV (Closed-Circuit Television) and sensor based intelligent surveillance systems have attracted considerable attentions in the field of public security affairs. To provide real time reaction in the case of a huge volume of the surveillance data, researchers have proposed event reasoning frameworks for modelling and inferring events of interest. However, they do not support decision making, which is very important for surveillance operators. To this end, this paper incorporate a function of decision making in an event reasoning framework, so that our model not only can perform event reasoning but also can predict, rank, and alarm threats according to uncertain information from multiple heterogeneous sources. In particular, we propose a multi-attribute decision making model, in which an object being watched is modelled as a multi-attribute event, where each attribute corresponds to a specific source, and the information from each source can be used to elicit a local threat degree of different malicious situations with respect to the corresponding attribute. Moreover, to assess an overall threat degree of an object being observed we also propose a method to fuse the conflict threat degrees regarding all the relevant attributes. Finally, we demonstrate the effectiveness of our framework by an airport security surveillance scenario.

Keywords: multi-attribute decision making, uninorm, decision making under uncertainty, event modelling and reasoning, D-S theory of evidence, ambiguity, surveillance systems.

1. INTRODUCTION

Due to the increasing threats of terroristic and criminal behaviours in the present world, researchers have developed lots of intelligent surveillance systems, such as suspect object tracking[14,19,34,46], intrusion detection[4,54], indoor security systems[52,65], traffic safety analysis[51,61,70], anti-social behaviour analysis[3,7,48], and so on. The primary aim of these studies is to develop security system that can detect and predict the potential threats of objects being watched according to a large collection of meaningful events that are derived from sensory data of dispersed sources. To proactively utilise the large amount of basic events in surveillance applications, obviously these events should be analysed in real-time, so a built-in event reasoning system is in need. Thus, researchers developed plenty of event modelling and reasoning systems[1,26,56], which can predict well threats or actions that may lead to devastating consequences. However, to date few of them have studied event modelling and reasoning

‡The corresponding Author e-mail: luoxd@mailbox.gxnu.edu.cn.
¶The corresponding Author e-mail: ycjiang@scnu.edu.cn

together with the decision making problem: how to rank the potential threats of multiple objects being watched, and select some of them to carry out further appropriate actions (*e.g.*, preventing the action of a suspect immediately, stop monitoring to some suspects, and so on) according to uncertain and conflicting information from different sources?

This decision making problem is extremely important because in reality the security operator often has to make decisions in the case that the security resources are limited[11] but plenty of malicious behaviours happen simultaneously. For example, several event concerning security could happen simultaneously during 21:00 to 21:15 in an airport:

- In the shopping area, a person (ID: 13) loiters near a foreign currency exchange shop from 21:03 to 21:15. Also, camera 42 captures the person's back image at the entrance of the shopping area at 21:01 and camera 45 captures the person's side face image at the foreign currency exchange shop from 21:03 to 21:15.
- In the control centre, at 21:03, the face of a person (ID: 19) appears in camera 29 in the middle of the corridor to the control centre at 21:03. Unfortunately, the person's face is not recorded by camera 23 (which is monitoring the entrance to the corridor). In other words, it means the person may be illegally infiltrating the control centre.

Support that a system can recognise age, gender, and behaviour, and then re-acquire objects being watched when necessary, and at that time period there is only one security team available. Then, the system needs to distinguish the potential threat degree of each object being watched and selects the one with the higher potential threat to deal with. In other words, the system needs to rank the potential threats according to the following two factors:

(i) Belief (*i.e.*, what the system believes). For example, if a person enters a security zone in an airport with its back facing the camera, the person may be classified as a *male* with a certainty of 65% by a gender classification algorithm. This is the uncertain belief of the system on the person's gender.
(ii) Utility (*i.e.*, what the system assesses). That is, the preference degree of the states of interest according to the mission of the system. In a surveillance system, since it is designed to identify and prevent threats, such a state can be about a person's gender, emotion, intention, and so on. In the example that a person enters a security zone in the airport, regarding the person's gender, the state of *male* should be more aggressive than that of *female*. Accordingly, the threat degree of a male object should be higher than that of a female (statistics have been consistent in reporting that men commit more criminal acts than women[12,62]).

Moreover, in reality an event can be detected at the same time by different sensor technologies, including audio, video, and other types of sensors (even including humans). Hence, important is how to fuse the information from multiple sensors regarding the same object to obtain an overall assessment of its potential threat. A typical scenario is that a camera in a security zone detects an unknown male (thus relatively higher potential threat); while the personnel authentication identification system strongly indicates the person just is a new staff (thus relatively low potential threat). In this case, should the system assign the object with a high threat degree or a low threat degree? A reasonable method for handling this problem is to consider a number of independent attributes (*e.g.*, gender, age, ID, and behaviour) to individually rate the potential threat of an object from the system's local perspective (what it believes and what it assesses), and then aggregate these local assessments to an overall one. Thus, since these local assessments are not completely consistent and the priorities of attributes concerned are different, an adequate weighted aggregation operator is required in order to obtain the overall assessment.of potential threat for each watched object and resolve the inconsistent or conflicting threat assessments of the watched objects in surveillance.

Therefore, in this paper we propose an integrated framework for event reasoning and decision making for distributed intelligent surveillance systems. More specifically, based on Dempster-Shafer (D-S) theory of evidence[55], we first propose a model of the multi-attribute

event under uncertainty. Then we use a normalised version of the Hurwicz's attribute[20] to obtain the degree of potential threat of each watched object with respect to each attribute. Finally, according to some intuitions in surveillance, we use a specific weighted uninorm aggregation operation[63,36,35] to obtain the overall degree of potential threat for each suspect after considering all relevant attributes, from which the priority for monitoring each object can be derived.

This paper advances the state of the art in the area of intelligent surveillance systems in the following aspects. (i) We identify two factors that influence the potential threats of objects being watched in a surveillance system: belief and utility. (ii) We propose an event model to estimate the potential threats of suspects based on multiple sources with heterogeneous, uncertain information. (iii) We develop a decision support model to reduce the burden of exhaustive event-rule structures, which is inefficient for large scale threat prevention problems. (iv) We integrate the event reasoning with a decision support model for distributed intelligent surveillance systems, using a multi-attribute fusion architecture.

The rest of this paper is organised as follows. Section 2 recaps D-S theory and the event modelling framework. Section 3 discusses the basic requirements for an appropriate multi-attribute event reasoning framework with decision support. Section 4 presents our multi-attribute event model. Section 5 develops a decision support model with an aggregation operator to handle the problem of judging the levels of potential threats for multiple suspects. Section 6 illustrates the effectiveness of our model. Section 7 discusses related work. Finally, Section 8 concludes this paper with future work.

2. PRELIMINARIES

This section recaps some basic concepts in D-S theory of evidence.

Dempster and Shafer[18,55] extend the concept of probability to the following one:

Definition 1. *Let Θ be a set of exhaustive and mutually exclusive elements, called a frame of discernment (or simple a frame). Mapping $m : 2^{\Theta} \to [0,1]$ is a mass function if $m(\emptyset) = 0$ and $\sum_{A\subseteq\Theta} m(A) = 1$.*

Since the sources where relevant evidence comes from may not be completely reliable in reality, Lowrance, Garvey, and Strat[33] introduce the concept of *Discount rate*, by which a mass function can be discounted to reflect the reliability of evidence:

Definition 2. *Let m be a mass function over a frame of discernment Θ and τ ($0 \leq \tau \leq 1$) be a discount rate to reflect the reliability of the source, where the evidence that the mass function reflects is from. In particular, when $\tau = 0$, the source is absolutely reliable; and when $\tau = 1$, the source is totally unreliable. Then the discounted mass function, denoted as m_τ, is given by:*

$$m_\tau(A) = \begin{cases} (1-\tau)m(A) & \text{if } A \subset \Theta, \\ \tau + (1-\tau)m(\Theta) & \text{if } A = \Theta. \end{cases} \tag{1}$$

Once a mass function has been discounted, it is then treated as fully reliable.

D-S theory of evidence also provides a rule to combine several mass functions that reflect multiple pieces of evidence from different kinds of independent sources as follows:

Definition 3. *Let m_1 and m_2 be two mass functions from independent and fully reliable sources over a frame of discernment Θ. Then the combined mass function of m_1 and m_2 by* Dempster's combination rule*, denoted as $m_{1,2}$, is defined as:*

$$m_{1,2}(x) = \begin{cases} 0 & \text{if } x = \emptyset, \\ \frac{\sum_{A\bigcap B=x} m_1(A)m_2(B)}{1-k} & \text{if } x \neq \emptyset, \end{cases} \tag{2}$$

where normalisation constant

$$k = \sum_{A_i \bigcap B_j = \emptyset} m_1(A) m_2(B) \tag{3}$$

is a measure of the conflict between the pieces of evidence in the combination.

Finally, in order to transmit the belief distributions from preconditions to the conclusion in an inference rule, Liu, Hughes, and McTear[32] propose a modelling and propagation approach based on the notion of evidential mapping as follows:

Definition 4. $\Gamma^* : 2^{\Theta_E} \to 2^{2^{\Theta_H} \times [0,1]}$ *is an evidential mapping, which establishes the relationship between two frames of discernment* Θ_E *and* Θ_H*, if* Γ^* *assigns a subset* $E_i \subseteq \Theta_E$ *to a set of subset-mass pairs in the following way:*

$$\Gamma^*(E_i) = \{(H_{i1},\ f(E_i \to H_{i1})),\ \ldots,\ (H_{it},\ f(E_i \to H_{it}))\}, \tag{4}$$

where $H_{ij} \subseteq \Theta_H$ *(*$i \in \{1,\ \ldots,\ n\}$*,* $j \in \{1,\ \ldots,\ t\}$*) and* $f : 2^{\Theta_E} \times 2^{2^{\Theta_H}} \to [0,\ 1]$ *satisfy:*

(i) $H_{ij} \neq \emptyset$*;*

(ii) $f(E_i \to H_{ij}) \geq 0$*;*

(iii) $\sum_{j=1}^{t} f(E_i \to H_{ij}) = 1$*;*

(iv) $\Gamma^*(\Theta_E) = \{(\Theta_H, 1)\}$.

Therefore, a piece of evidence on Θ_E can be propagated to Θ_H through evidential mapping Γ^* as follows:

$$m_{\Theta_H}(H_j) = \sum_i m_{\Theta_E}(E_i) f(E_i \to H_{ij}). \tag{5}$$

3. REQUIREMENTS ANALYSIS

In this section, we analyse some basic requirements that an appropriate multi-attribute event reasoning framework with decision support should meet.

(i) *The uncertainty of event recognition.* The reason why video sensors cannot provide complete, accurate information for a scenario evolving over time is that an event recognised by a video analysis algorithm may be uncertainty. For instance, it could be very difficult for a system to judge a person is a male or female when the camera just captures the back of the person. Therefore, an intelligent multi-attribute surveillance system should be able to represent and infer useful information with uncertainty. Moreover, in this case, the person may be classified as a *male* with the certainty of 65% by a gender classification algorithm. Nevertheless, it does not mean that the remaining 35% should simply be classified as female. Perhaps it is unknown how to distribute the certainty of 35% on male or female. In order to handle the ambiguous information, we employ D-S theory of evidence. Along with this challenge comes the issue of *reliability* of sources. That is, when a classification algorithm is used to detect an event that is not 100% accurate itself, how to intergrade the reliability of the algorithm with the detected events (which are uncertain)?

(ii) *The discrimination between threat degree and belief of threat.* The main goal of the intelligent surveillance system is to detect and prevent the potential threat of suspects based on a sensor network. However, due to the uncertainty of recognised events, to achieve the goal the system needs to consider the threat degree of an abnormal behaviour as well as the belief that such a potential threat happens. For instance, in an airport scenario, a surveillance system

detects, with a very high belief degree, that two young people are fighting in the shopping area, and at the same time, with a medium belief degree, that a person has left a bomb in airport terminal 1. In this case, an appropriate multi-attribute event reasoning framework with decision support should be able to determine the priorities of these two cases when only one security team is available at that moment.

(iii) *The independence of the threat assessments regarding multiple classification algorithms.* In the airport surveillance scenario we gave in Section 1, since usually the classification algorithms of the surveillance system can just provide uncertain information regarding more than one attribute (*i.e.*, watched object's age, gender, behaviour, and watched object re-acquisition), the event model must reflect all of the information for further reasoning and decision making. Nevertheless, since an output from a sensor-data classification algorithm focuses on a single attribute and the information provided by each classification algorithm is concerned with two aspects (*i.e.*, threat degree and belief of threat) as mentioned in Challenge (ii), it is difficult to give an overall threat assessment of a watched object by an event that considers the effect of all the relevant attributes without an aggregation method. Therefore, a definition is required for multi-attribute event modelling.

(iv) *The efficiency of decision support.* In reality, most of malicious behaviours occur in a short period of time. As a result, the surveillance system has to be able to make a decision rapidly to prevent the potential threat.

(v) *The criticality of event for threat assessment.* A CCTV-based surveillance system may need to handle events in different places at different time points, so the extent of attention on a given event should be different after considering the spatial-temporal background information. For instance, an event that happened in an area with high crime statistics at midnight should be more critical than an event that happened in an area of low-crime statistics in the morning. The higher the criticality of the events, the more attention the security team should pay. Thus, the multi-attribute event modelling and reasoning framework with decision support should reflect the property in threat assessment.

(vi) *The conflict of multiple threat assessments.* A CCTV-based surveillance system could consist of hundreds of cameras and a number of algorithms to classify the characteristics of interest for a given watched object in, for example, a medium-size airport. Thus, according to different cameras/sensors or different classification algorithms, the assessment of the potential threat of the watched object could be conflicting. Typically, from a camera in a security zone a strange male is detected (higher threat), but the personnel authentication identification system strongly indicates the person is a new staff (lower threat). As a result, we need a proper method to resolve this conflict.

(vii) *The assessment aggregation of potential threat.* A straightforward method to handle a multi-attribute threat assessment problem in a surveillance system use a number of independent attributes (*e.g.*, gender, age, ID, and behaviour) to individually assess the potential threat of a watched object, and then to combine these individual assessments to gain an overall assessment. Since these individual assessments cannot always be completely consistent and the priorities of these attributes could be different, we need an adequate aggregation operator to obtain the overall assessment of the potential threat degree of each watched object and resolve the inconsistency or conflict between them.

Actually, the above seven challenges reflect the basic requirements for our multi-attribute event modelling and reasoning framework with multi-attribute decision support. To take challenge (i), we can associate a mass function to an event to reflect its uncertainty, and put the influence of the reliability degree of the sensors into account as well. To take challenge (ii), regarding the independence of multiple classification algorithms, we make it clear that each atomic event should be related to one classification algorithm only. That is, an atomic event regards only one of attributes. To take challenge (iii), we need to define a utility function on the state set of each attribute. For instance, for the attribute *gender*, possible states *male* and *female* should be mapped to a utility value to reflect their threat degrees. To take challenge (iv), a decision making model is required. To take challenge (v), we will propose a threat

assessment method that considers the significance of an event with respect to each attribute. Finally, to take challenges (vi) and (vii) we will propose an aggregation operator to give an overall threat assessment based on the threat assessment of each attribute. These are the content of the following two sections.

4. EVENT REPRESENTATION AND REASONING

In this section, we will define multi-attribute events and their reasoning rule.

First, we discuss the formal definition of an atomic event. Intuitively, a specific event definition should be determined by a real-world surveillance application for all the attributes concerned. Moreover, some common attributes should be held in order to construct an atomic event for detecting the potential threat of objects being watched. Formally, we have:

Definition 5. *An atomic event e for detecting the potential threats is a tuple*

$$(T_e, t_e, loc, ID_s, c, ID_p, d_{sr}(ID_s), d_{es}(t, loc), w_c, m_c, u_c),$$

where:

(i) T_e *is the type of event* e*;*

(ii) t_e *is a time interval during which event* e *is observed;*

(iii) loc *is the location of a source from which event* e *is detected;*

(iv) ID_s *is the identification of a source from which event* e *is detected;*

(v) c *is one of the attributes that are used to assess potential threats for a watched object;*

(vi) ID_p *is the identification of a watched object/person from which event* e *is detected;*

(vii) $d_{sr}(ID_s)$ *is the degree of reliability of source* ID_s*, which is obtained by a reliability function* $r : S \to [0, 1]$*, where* S *is the set of sources and* $ID_s \in S$*;*

(viii) $d_{es}(t, loc)$ *is the degree of criticality of event* e *based on background knowledge defined by the location and time event* e *happened at, which is obtained by a criticality function* $d_{es} : T \times L \to [0, 1]$*, where* T *is the set of time points, and* L *is the set of the locations of the sensors with* $loc \in L$*;*[*]

(ix) w_c *is the importance degree of an attribute* c *in terms of determining a potential threat of event* e*, obtained by* $w : C \to [0, 1]$*, where* C *is the set of attributes that can be detected by the sensor network and* $c \in C$*;*

(x) $m_c : 2^{\Omega_c} \to [0, 1]$ *is a mass function over the set of possible states of a given attribute* c *to represent the uncertain results of a classification algorithm of the sensor related to event* e*; and*

(xi) $u_c : \Omega_c \to \Theta$ *is a utility function over the set of possible states of a given attribute* c *to represent the threat degree of a state, where* $\Theta = \{h_i \mid h_i \in \mathbb{R}, i = 1, \ldots, n\}$*.*

The following is an example of atomic events.

[*]Here, for a time interval, we will consider the time point t with the highest significance degree.

Example 1. *Suppose we are monitoring some people passing an airport security area. Then an atomic event could be*

$$e_g = (PPSA, 18{:}03\text{–}18{:}05, ASA1, 43, gender, 12, 0.9, 0.8, 0.3, (m_g(\{male\}) = 0.7, m_g(\{male, female\}) = 0.3), u_g).$$

That is, for an event with type PPSA (Person Passing Security Area) at 18:03–18:05, in Airport Security Area 1 (ASA1) sensor 43 *detects the gender of the watched object with ID* 12 *by the corresponding classification algorithm, the reliability degree of the sensor is* 0.9*, the criticality of this event is* 0.8*, and the weight of attribute gender for detecting a potential threat is* 0.3*. Moreover, the watched object is recognised as male with a certainty of* 70%*, and* 30% *that the gender of the watched object is not clearly known. Finally, the level of potential threat for each state of the gender attribute (i.e., male or female) is given by utility function* u_g*.*

There might be a set of events with the same attribute, watched objects' IDs, and event type but different source IDs or observed time points or locations. For example, a person (with watched object ID 12) broads a bus with its back facing camera 1 at 21:15 and then sits down with its side face detected by camera 2 at 21:20. Suppose the gender classification algorithm indicates that $m_g^1(\{male\}) = 0.5$ and $m_g^1(\{female,\ male\}) = 0.5$ by the data from camera 1, and $m_g^2(\{male\}) = 0.7$ and $m_g^2(\{female,\ male\}) = 0.3$ by the data from camera 2. Since they refer to the same attribute about the same watched object in the same case from different sources, we need to combine these two events to figure out the gender of the watched object. In our model, the combination of events is realised by Dempster's combination rule on discounted mass functions. That is, first we use formula (1) to obtain the discounted mass functions based on the value of $d_{sr}(ID_{s,i})$ (*i.e.*, the reliability of source with ID i); and then we use formula (2) to combine the discounted mass functions. Here, since we have defined that events can have a time duration, events in an event flow with a time duration shares one mass function.

Now we consider the event reasoning in our framework. Since in our model we only care about the decision support issue based on the potential threat of the suspects, we just give a set of inference rules which focus on the meaningful event (*i.e.*, the event relevant to a potential threat). More specifically, we have:

Definition 6. *An inference rule in our framework is defined as a tuple* $(T_e, Condition, m_{IET}, u_{IET})$*, where:*

(i) T_e *is the type of event;*

(ii) Condition is a conjunction of a set of conditions for selecting related events from the event flow to infer another event;

(iii) m_{IET} *is a mass function for the possible intention of a watched object; and*

(iv) u_{IET} *is a utility function presenting what the system desires.*[†]

In the above definition, since m_{IET} is a mass function over a set of exhaustive and mutually exclusive elements, it can be defined over two different kinds of frames of discernment: (i) a frame of discernment about the possible intention of a watched object; and (ii) a frame of discernment about the potential threat: {*Has Threat, Has No Threat*}. And when analysing events with multiple attributes, the criticality of an event, the weight of different attributes, the possible states of each attribute, and so on should all contribute to the assessment of potential threats. Thus, it is unreasonable to ask experts to directly assign the degree of a potential threat without any knowledge about the factors that contribute to the threat. In contrast, the values of possible intentions of a watched object can be easily obtained by some historical data,

[†]We will discuss more details about utilities in next section.

some pattern recognition algorithms or the judgments of experts directly. For example, m_{IET} for the event inference rule about loitering in a ticker counter is over a frame $\{Rob, Waiting\ Friends\}$. And we divide behaviours into different categories, such as movements, relations with objects, relations with peoples, hand actions (*e.g.*, to detect a fight), and so on.

Moreover, by the above definition, we can infer watched objects' intentions just according to their behaviours because of several reasons. First, many social psychology studies have revealed that humans can infer the intentions of others through observing their behaviours [8,23]. Nonetheless, it lacks strong evidence to support that people's intentions are directly concerned with their age, gender, and emotion, especially when we desire to infer the malevolence intention of the watched objects to assess their potential threat. So, to reduce the complexity of constructing the inference rules, we do not consider other attributes except the behaviour of the watched objects in inferring their intentions. Second, in a multi-attribute surveillance environment, it could be very difficult for a security expert to assess the possibility of various intentions of a watched object regarding multiple attributes. For example, it is easy for an expert to assess the intention of a person who loiters at a ticket counter since the expert just needs to consider the relation between a certain behaviour (*e.g.*, loitering) and different intentions; but if the expert considers three attributes of age, gender, and behaviour, somehow it is difficult to figure out who (*e.g.*, an unknown age man or a young unknown gender person, both loitering at a ticket counter) has a higher chance to rob. Third, by distinguishing the effect of each attribute for the degree of potential threat separately, our definition considers the criticality function of an event and the weights of attributes in contributing to the assessment of potential threats to a given target. We will discuss these issues in details in the next section.

The following is an example for the event inference rule in our model about the intention of a watched object in the shopping area at an airport:

Example 2. *The rule describing that a person loitering in the Foreign Currency Exchange (FCE) shop at an airport could be suspicious can be defined as (T_e, Condition, w_{IPL}, m_{IPL}, u_{IPL}), where:*

- *T_e is IPL (Intention of Person Loitering) in the foreign currency exchange shop;*
- *Condition is defined as:*

$$(m_i^m(\{loiter\}) > 0.5) \wedge (loc = \textit{the foreign currency exchange shop}) \wedge (t_{e,n} - t_{e,0} > 10\ \textit{minutes});^{\ddagger}$$

- *w_{IPL} is 0.8;*
- *m_{IPL} over a frame $\{Rob\ (R), Waiting\ for\ Friends\ (WF)\}$ is specified by:*

$$m_{IPL}(\{R\}) = 0.5, m_{IPL}(\{WF\}) = 0.3, m_{IPL}(\{R, WF\}) = 0.2;$$

- *u_{IPL} is given by:*

$$u_{IPL}(Rob) = 9,\ u_{IPL}(Wait\ for\ Some\ Friends) = 3.$$

5. FINDING THE MOST DANGEROUS THREAT

The previous section developed a multi-attribute event representation and reasoning model. Thus, by inference rules and classification algorithms, the system can provide non-deterministic identification results. So, we need to describe the multiple possible states by mass values. For instance, in Example 1, e_g means that the person with ID 12 passing security area at 18:03–18:05 is a male with a certainty degree of 70% by a classification algorithm with ID 43; and in Example 2, the inferred event of e_{IPL} with $m_{\text{IPL}}(\{Rob\}) = 0.5$ means that by the rule in Example 2, a watched object who satisfies the condition of the rule has a possibility of 50% to undertake a robbery. Actually, the instantiated attribute with a state and a mass value reflects the belief of the system: to which degree a given state of the attribute could happen.

However, in real world, multiple events could be identified at the same time by different sensors, whilst those events might not be at the same level of potential threats. As a result, what the system believes is not enough to rank the relative importance of different suspects. For example, given a bomb attacker with a low certainty and a drunk troublemaker with a high certainty, the system should be able to determine which one should be pay more attention. Thereby, to rank the threats, we have to consider which threat is the most dangerous one. That is, we need to define the threat degree as a utility of each state regarding an attribute. With the threat degree and the mass value for each possible state, we can finally calculate its potential threat, and report the watched object with high potential threats. Now, combining what the system believes (mass values of states) and what the system values (utilities), the problem of detecting potential threats can be viewed as a decision problem: how to rank the potential threat of each watched object properly? That motivates us to construct a decision support system that can automatically rank watched objects in a multi-attribute surveillance environment under uncertainty by the utility (the degree of potential threat) and the mass function of different possible states of each attribute in this section.

5.1. Calculation of potential threat degree regarding each attribute

In this subsection, we will propose a method to calculate the degrees of potential threats regarding each attribute.

Semantically, by Definition 5, the degree of potential threat (*i.e.*, the utility of the states) can be represented by substituting the frame of discernment Ω_c for each attribute by a frame of discernment $\Theta = \{h_1, ..., h_n\}$, where each h_i is a real number that has one-to-one correspondence with a state in Ω_c. For example, suppose the two gender states are ranked in a 10-level (*i.e.*, 1-10, with 10 as the highest level and 1 as the lowest level) potential threat, and in particular male is ranked 6 and female is ranked 4 (meaning that a male has a stronger potential threat than a female). Then $\Omega_c = \{$*male, female*$\}$ will be substituted by a frame of discernment $\Theta = \{6, 4\}$. Obviously, this direct substitution process does not change the mass values for states or the number of elements in Ω_c. Moreover, since humans can infer the intentions of others through observing their behaviours[8,23], the attribute of behaviours should be used in rules by the event inference system to predict the intention of the watched objects. Here note that it is the person's intention, rather than his/her behaviour, that determines his/her potential threat. Therefore, utilities are only concerned with the inferred events, reflecting people's intention, but not directly with the events of behaviours.

Hence, based on the mass function and the utility of states, we can obtain the expected utility interval for the expected degree of potential threat by extending the Start's method[58] as follows:

Definition 7. *For a watched object with ID x with respect to a given attribute c specified by mass function $m_{c,x}$ over $\Theta = \{h_1, ..., h_n\}$, where h_i is a real number indicating the utility (potential threat degree) of each possible value of attribute c, its expected utility interval (interval of expected potential threat degree) is $EUI_c(x) = [\underline{E}_c(x), \overline{E}_c(x)]$, where*

$$\underline{E}_c(x) = \sum_{A \subseteq \Theta} m_{x,c}(A) \min A, \tag{6}$$

$$\overline{E}_c(x) = \sum_{A \subseteq \Theta} m_{x,c}(A) \max A. \tag{7}$$

After the system obtains the expected utility interval, we can apply the following principle to find the point-valued degree of potential threat regarding each attribute:

Definition 8. *Let $EUI_c(x) = [\underline{E}_c(x), \overline{E}_c(x)]$ be an interval-valued expected degree of potential threat of attribute c for watched object with ID x, $\delta_c(x) = d_{es}$ be the criticality function for the events based on the background information by Definition 5, and n be the highest level of potential threat, then the point-valued degree of potential threat of the watched object with ID*

x with respect to attribute c is given by:

$$\nu_c(x) = \frac{(1-\delta_c(x))\underline{E}_c(x) + \delta_c(x)\overline{E}_c(x)}{n}. \tag{8}$$

Actually, this definition is a normalised version of the Hurwicz criterion [20]. That is, n is a normalisation factor to make sure that the point-valued degree of potential threat is in the range of $[0, 1]$. The following theorem reveals the relation between the criticality function and the point-valued degree of potential threat:

Theorem 1. *Let $EUI_c(x) = [\underline{E}_c(x), \overline{E}_c(x)]$ be an interval-valued expected degree of potential threat of the watched object with ID x regarding attribute c, $\delta_c(x)$ and $\delta'_c(x)$ be the degrees of criticality of the events in two different backgrounds respectively, $\delta_c(x) \geq \delta'_c(x)$, and n be the highest level of potential threat. Then $\nu_c(x) \geq \nu'_c(x)$.*

Proof
By formula (8), $\delta_c(x) \geq \delta'_c(x)$, and since $\overline{E} \geq \underline{E}$, we have:

$$\begin{aligned}\nu_c(x) - \nu'_c(x) =& \frac{(1-\delta_c(x))\underline{E}_c(x) + \delta_c(x)\overline{E}_c(x)}{n} - \frac{(1-\delta'_c(x))\underline{E}_c(x) + \delta'_c(x)\overline{E}_c(x)}{n} \\ =& \frac{(\delta_c(x) - \delta'_c(x))(\overline{E}_c(x) - \underline{E}_c(x))}{n} \\ >& 0.\end{aligned}$$

□

By Theorem 1, since $\delta_c(x) = d_{es}$, we can find that the point-valued degree of potential threat with respect to each attribute for the watched objects is higher if the set of events happen in an area with high crime statistics in midnight than that if the set of events happen in a lower crime area in morning.

The following theorem implies that Definition 8 captures some intuitions well.

Theorem 2. *Let $EUI_c(k) = [\underline{E}_c(k), \overline{E}_c(k)]$ be an interval-valued expected degree of potential threat of the attribute c for the watched object with ID k, $\delta_c(k)$ be the degrees of criticality of the event involving the watched object with ID k, and n be the highest level of potential threat. Then the point-valued degrees of potential threat for these two watched objects satisfy:*

(i) if $\underline{E}_c(x) > \overline{E}_c(y)$, then $\nu_c(x) > \nu_c(y)$; and

(ii) if $\underline{E}_c(x) > \underline{E}_c(y)$, $\overline{E}_c(x) > \overline{E}_c(y)$, and $\delta_c(x) \geq \delta_c(y)$, then $\nu_c(x) > \nu_c(y)$.

Proof
(i) By $\delta_c(k) \in [0, 1]$ ($k \in \{x, y\}$), we have

$$\underline{E}_c(k) \leq (1-\delta_c(k))\underline{E}_c(k) + \delta_c(k)\overline{E}_c(x) \leq \overline{E}_c(k).$$

Then, by Definition 8, we have

$$\frac{\underline{E}_c(k)}{n} \leq \nu_c(k) \leq \frac{\overline{E}_c(k)}{n}.$$

Thus, by $\underline{E}_c(x) > \overline{E}_c(y)$, we have

$$\nu_c(x) - \nu_c(y) \geq \frac{\underline{E}_c(k)}{n} - \nu_c(y) \geq \frac{\underline{E}_c(k) - \overline{E}_c(y)}{n} > 0.$$

So, item (i) holds.

Table I. The notations of our model

Notation	Interpretation
$\nu_i(x)$	DPT of watched object x for attribute i
w_i	the degree of importance for an attribute w_i
$g(w_i, \nu_i(x))$	weighted DPT
$R(g(w_i, \nu_i(x)), g(w_j, \nu_j(x)))$	Combined assessment of $g(w_i, \nu_i(x)$ and $g(w_j, \nu_j(x))$
$e \in (0, 1)$	the threshold to distinguish different combination attitudes

(ii) When $\underline{E}_c(x) > \underline{E}_c(y)$, $\overline{E}_c(x) > \overline{E}_c(y)$, and $0 \leq \delta_c(y) \leq \delta_c(x) \leq 1$, we have

$$\begin{aligned}
\nu_c(x) - \nu_c(y) =& \frac{(1-\delta_c(x))\underline{E}_c(x) + \delta_c(x)\overline{E}_c(x)}{n} - \frac{(1-\delta_c(y))\underline{E}_c(y) + \delta_c(y)\overline{E}_c(y)}{n} \\
=& \frac{(\underline{E}_c(x) - \underline{E}_c(y)) + \delta_c(x)(\overline{E}_c(x) - \underline{E}_c(x)) - \delta_c(y)(\overline{E}_c(y) - \underline{E}_c(y))}{n} \\
\geq& \frac{(\underline{E}_c(x) - \underline{E}_c(y)) + \delta_c(x)(\overline{E}_c(x) - \underline{E}_c(x)) - \delta_c(x)(\overline{E}_c(y) - \underline{E}_c(y))}{n} \\
=& \frac{(1-\delta_c(x))(\underline{E}_c(x) - \underline{E}_c(y)) + \delta_c(x)(\overline{E}_c(x) - (\overline{E}_c(y))}{n} \\
>& 0.
\end{aligned}$$

So, item (ii) holds. □

In fact, Theorem 2 exhibits two intuitions concerning the point-valued degrees of potential threat of any two suspects: (i) for a given attribute, if the lowest expected degree of potential threat of a suspect is higher than the highest expected degree of potential threat of another suspect, the point-valued degree of potential threat of the first one should higher; and (ii) if the criticality function for the events of a suspect is not more than that of the other, and the lowest and highest expected degrees of potential threat of this suspect are higher than those of the other respectively, the point-valued degree of potential threat of this one should higher.

5.2. A weighted aggregation operator

After obtaining the point-valued degree of potential threats of the watched objects regarding each attribute, in order to rank the potential threats of all the suspects to take the appropriate action directly, in this subsection we will discuss how to use a weighted aggregation operator[41,39,63] to calculate the overall degree of a potential threat for each watched object after considering all relevant attributes. And Table I lists notations used in Ma *et al.*'s paper[41], where DPT (Degree of Potential Threat) involves a given attribute for watched object x.

Specifically, we use the following weighted aggregation operator the overall degree of potential threat regarding any two attributes 1 and 2 as follows:

$$\begin{aligned}
& R(g(w_1, \nu_1(x)), g(w_2, \nu_2(x))) \\
=& \frac{(1-\tau)g(w_1, \nu_1(x))g(w_2, \nu_2(x))}{(1-\tau)g(w_1, \nu_1(x))g(w_2, \nu_2(x)) + \tau(1 - g(w_1, \nu_1(x)))(1 - g(w_2, \nu_2(x)))},
\end{aligned} \tag{9}$$

where τ is the threshold value to distinguish different types of attribute and

$$g(w_i, \nu_i(x)) = w_i\nu_i(x) + (1 - w_i)\tau. \tag{10}$$

Formula (9) is obtained by integrating the following specific uninorm aggregation operator[36,35]:§

$$R(x,y) = \frac{(1-\tau)xy}{(1-\tau)xy + \tau(1-x)(1-y)} \tag{11}$$

as shown in Luo et al.'s work[36,35] with weighting function (10)[63].

The reason why we suggest to employ the weighted uninorm that it satisfies all the following basic principles that a threat assessment aggregation needs to follow, as argued by Ma, Liu, and Hong[41]:

(i) Conclusion modification: Consider one more threat assessment for a given watched object regarding a new attribute can increase, or decrease, or remain the current assessment.

(ii) Assessment consistency: The overall potential threat assessment for a given watched object should increase when the point-valued degree of potential threat of a watched object regarding each relevant attribute increases.

(iii) Assessment commensurability: A system needs to provide an overall assessment for each watched object after the aggregation process, and the overall assessments for different watched objects are comparable (on a commensurable scale).

(iv) Irrelevance of evidence ordering: The result of an aggregation should not be affected by the ordering of aggregation.

(v) Importance dependency: The overall assessment depends on the importance (reflected as a weight) of each attribute.

Moreover, the aggregation operator in formula (10) also has some desired properties[63]: (i) monotonicity: if $x_1 \geq y_1 \wedge x_2 \geq y_2$ then $R(x_1, x_2) \geq R(y_1, y_2)$; (ii) boundary conditions: $R(0,0) = 0$ and $R(1,1) = 1$; (iii) associativity: $R(R(x_1, x_2), x_3) = R(x_1, R(x_2, x_3))$; (iv) symmetry: $R(x_1, x_2) = R(x_2, x_1)$; and (v) neutral element: $\exists e \in (0,1), \forall x \in [0,1], R(e,x) = x$.

Finally, to rank the potential threats of watched objects according to their overall assessments, we introduce the concept of preference ordering as follows:

Definition 9. *For two watched objects x and y, the strict preference ordering $\succ$ is defined as:*

$$x \succ y \Leftrightarrow R(g(w_i, \nu_i(x)), \ldots, g(w_n, \nu_n(x))) > R(g(w_j, \nu_j(y)), \ldots, g(w_m, \nu_m(y))).$$

This preference ordering means that the potential threat of x is higher than that of y if and only if the overall threat assessment of x is greater than that of y. Hence, together with the equivalence relation $\sim$ (*i.e.*, $x \sim y$ if $x \not\succ y$ and $y \not\succ x$), we show that the preference ordering in Definition 9 is a total order that satisfies the properties of completeness and strict transitivity[41].

5.3. The whole picture of our event model with decision support

After obtaining the overall degree of a potential threat of each watched object after considering all the relevant attributes, now we can give the whole process of our event model with decision support in this subsection. First, using our event model with decision support, a security expert needs to determine: (i) the attributes' weights, (ii) the criticality function for different surveillance background, and (iii) the potential threat degree (utility) of each possible conclusion regarding different attributes.

§The concept of uninorm is introduced by Yager and Rybalov[63], and it is widely applied to many domains such as automated negotiation[36,37], fuzzy logic[28], market basket analysis[47], sequential decision making under uncertainty[21], fuzzy neural networks[17], and so on.

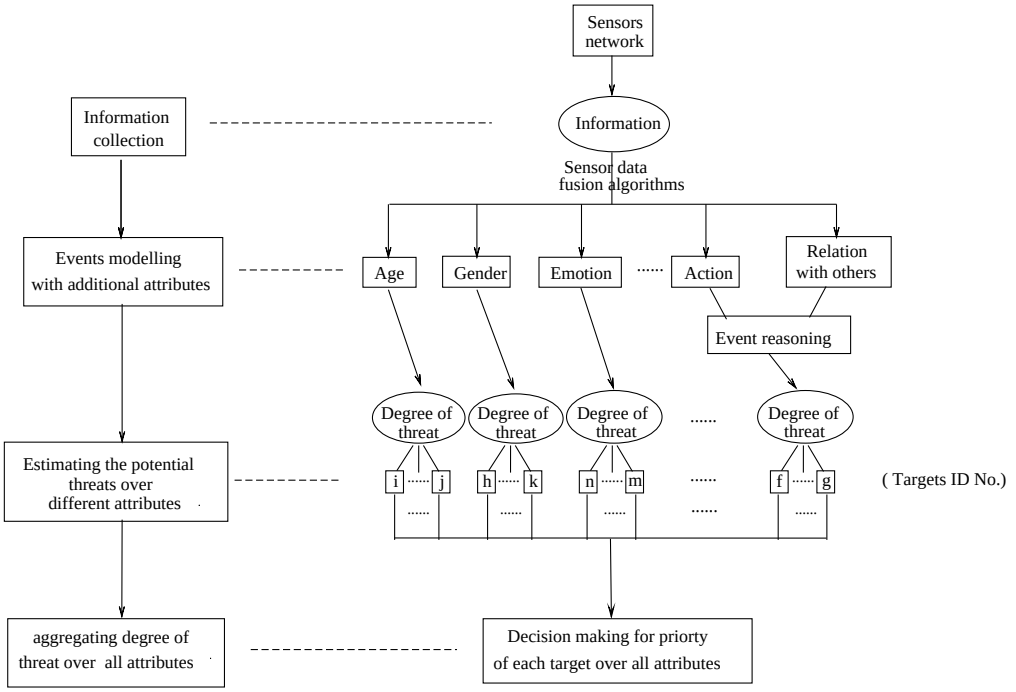

Figure 1. Procedure of our event model with decision support

Then, as shown in Figure 1, the procedure of our decision support framework is as follows. (i) Determine each watched object's possible relevant attributes based on the types of sensors and different classification algorithms. (ii) Define multiple attributes atomic events based on the the attributes weights, the criticality function for different surveillance background, the potential threat degree of each possible conclusion regarding different attributes, the information from different sensors, and algorithms for each watched object. (iii) Calculate the discount mass function according to the degree of reliability of the events for each watched object. (iv) Use Dempster combination rule to combine the discounted mass functions for the events with the same attribute for each watched object. (v) Obtain inferred events with respect to attribute *Intention* by the inference rules and the events with respect to any type of behaviour attribute. (vi) Calculate the potential threat degree of each watched object regarding each attribute (except all types of behaviour attribute) from the mass function and utility function. (vii) Use the weighted uninorm aggregation operator to obtain the overall degree of potential threat of each watched object from the potential threats regarding each attribute. And (viii) determine the preference ordering.

6. ILLUSTRATION

In this section, we use the airport security surveillance scenario can deal with real-world surveillance problems.

In the scenario, the surveillance system can rank the potential degree of each watched object as follows:

(i) The surveillance system detects the atomic events for each person as shown in Tables II and III based on the information of multiple sensors. For example, the first row in Table II means that for an event of type *SA* (shopping area) in FCE (the foreign currency exchange) shop at 21:01, the *age* classification algorithm used by camera 42 with reliability degree 0.9 detects a person with ID 13 as *young* with a certainty of 30%. The criticality of this event

Table II. Event modelling the airport security surveillance scenario (i)

Event	Type	Time	Location	Source ID	Criterion	Person ID	Reliability	Significance	Weight
e_a^{42}	SA	21:01	FEC	42	age	13	0.9	0.7	0.3
e_a^{45}	SA	21:03 -21:15	FCE	45	age	13	0.9	0.7	0.3
e_g^{42}	SA	21:01	FCE	42	gender	13	0.9	0.7	0.3
e_g^{45}	SA	21:03 -21:15	FCE	45	gender	13	0.9	0.7	0.3
e_m^{42}	SA	21:01	FCE	42	move	13	0.9	0.7	0.8
e_m^{45}	SA	21:03 -21:15	FCE	45	move	13	0.9	0.7	0.8
e_a^{29}	CC	21:03	MoC	29	age	19	1	0.9	0.3
e_g^{29}	CC	21:03	MoC	29	gender	19	1	0.9	0.3
e_{sr}^{23}	CC	21:03	MoC	23	sr	19	1	0.9	0.8

where SA means Shopping Area, FCE means Foreign Currency Exchange, CC means Control Centre, MoC means Middle of the Corridor.

Table III. Event modelling for the airport security surveillance scenario (ii), where $\Omega_m = \{walk\ to\ east, \ldots, walk, to\ north, loitering\}$ and the scale of measurement for the degree of potential threat is $\Theta = \{1, \ldots, 10\}$.

e	m_c	u_c
e_a^{42}	$m_{42,a}(\{young\}) = 0.3$, $m_{42,a}(\{young, old\}) = 0.7$	$u_a(young) = 6$, $u_a(old) = 2$
e_a^{45}	$m_{45,a}(\{young\}) = 0.6$, $m_{45,a}(\{young, old\}) = 0.4$	$u_a(young) = 6$, $u_a(old) = 2$
e_g^{42}	$m_{42,g}(\{female\}) = 0.4$, $m_{42,g}(\{female, male\}) = 0.6$	$u_g(male) = 6$, $u_g(female) = 4$
e_g^{45}	$m_{45,g}(\{male\}) = 0.7$, $m_{42,g}(\{female, male\}) = 0.3$	$u_g(male) = 6$, $u_g(female) = 4$
e_m^{42}	$m_{42,m}(\{walk\ to\ east, loitering\})=0.8$, $m_{42,m}(\Omega_m)=0.3$	determined by decision reference rules
e_m^{45}	$m_{45,m}(\{loitering\}) = 0.9$, $m_{45,m}(\Omega_m) = 0.1$	determined by decision reference rules
e_a^{29}	$m_{29,a}(\{young\}) = 0.7$, $m_{29,m}(\{young,\ old\}) = 0.3$	$u_a(young) = 6$, $u_a(old) = 2$
e_g^{29}	$m_{29,a}(\{male\}) = 0.7$, $m_{29,m}(\{male, female\}) = 0.3$	$u_g(male) = 6$, $u_g(female) = 4$
e_{sr}^{23}	$m_{23,sr}(\{unmatch\})=0.8$, $m_{23,m}(\{unmatch, match\})=0.2$	$u_{sr}(unmatch) = 9$, $u_{sr}(match) = 4$

is 0.7, the weight of attribute *age* for detecting a potential threat is 0.3, and u_a is the utility function that shows the degree of potential threat regarding attribute *age*.

(ii) Since some sensors are not completely reliable in our example, we obtain the discounted mass functions by formula (1). For example, regarding attribute *age* for the person in the foreign currency exchange shop, we have

$$m_{42,a,r}(\{young\}) = m_{42,a} \times d_{sr}(ID_{s,42}) = 0.3 \times 0.9 = 0.27,$$

and similarly we can obtain:

$$m_{42,a,r}(\{young, old\}) = 0.73,$$
$$m_{45,a,r}(\{young\}) = 0.54,$$
$$m_{45,a}(\{young, old\}) = 0.46.$$

(iii) We combine mass functions associated with events in different clusters (from different sources) where these events are all about a common attribute, using Dempster's rule in formula (2). For example, regarding attribute *age* for the person in the foreign currency exchange shop, we have

$$\begin{aligned}
&m_{42,45,a,r}(\{young\})\\
=&(m_{42,a,r}(\{young\}) \times m_{45,a,r}(\{young\}) + m_{42,a,r}(\{young\}) \times m_{45,a,r}(\{young, old\})\\
&+ m_{42,a,r}(\{young, old\}) \times m_{45,a,r}(\{young\}))/1\\
=&(0.27 \times 0.54 + 0.27 \times 0.46 + 0.73 \times 0.54)/1\\
=&0.664.
\end{aligned}$$

And similarity we can obtain

$$m_{42,45,a,r}(\{young, old\}) = 0.336.$$

Note that the mass function is associated with a derived event:

$$\begin{aligned}
e_a^{42\&45} =&(T_e, t_e, loc, ID_s, c, ID_p, d_{sr}(ID_s), d_{es}(t, loc), w_c, m_c, u_c)\\
=&(SA, 21{:}01\text{–}21{:}15, FCE, 42\&45, age, 13, 1, 0.7, 0.3,\\
&(m_{42,45,a,r}(\{young\}) = 0.664, m_{42,45,a,r}(\{young, old\}) = 0.336), u_a),
\end{aligned}$$

where $m_{42,45,a,r}$ is specified by the combination of the discounting mass function of e_a^{42} and the discounting mass function of e_a^{45}.

(iv) We conduct the event inference. For the movement of the person in the foreign currency exchange shop, by the similarly counting process of the discounted mass function and the combination of the mass functions for attribute *age* by formulas (1) and (2), we have:

$$m_{42,45,m,r}(\{walk\ to\ east,\ loitering\}) = 0.137,$$
$$m_{42,45,m,r}(\{loitering\}) = 0.81,$$
$$m_{42,45,m,r}(\Omega_m) = 0.053.$$

Then by the inference rule in Example 2 and formula (5), we have

$$\begin{aligned}
m_{\mathrm{IPL}}(\{Rob\}) =&m_{42,45,m,r}(\{loitering\}) \times f(\{loitering\} \to \{Rob\})\\
=&0.81 \times 0.5\\
=&0.41.
\end{aligned}$$

Similarly, we can obtain:

$$m_{\mathrm{IPL}}(\{Waiting\ for\ Friends\}) = 0.24,$$
$$m_{\mathrm{IPL}}(\{Rob,\ Waiting\ for\ Friends\}) = 0.35.$$

(v) We obtain the expected utility interval for each attribute of each person by Definition 7. For example, for the person with ID 13 in the foreign currency exchange shop, we have:

$$[\underline{E}_a, \overline{E}_a] = [4.656, 6];$$
$$[\underline{E}_g, \overline{E}_g] = [5.044, 5.656];$$
$$[\underline{E}_{\mathrm{IPL}}, \overline{E}_{\mathrm{IPL}}] = [5.43, 7.542].$$

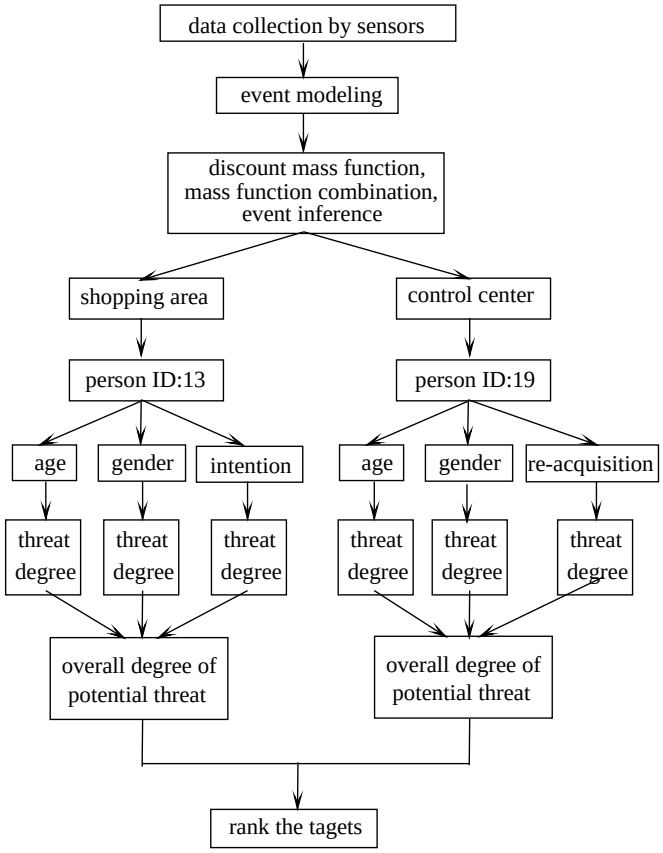

Figure 2. Process of the airport scenario

(vi) We calculate the point-valued degree of potential threat for each attribute of each person by Definition 8. For example, for the person with ID 13 in the foreign currency exchange shop, by formula (8), we have

$$\begin{aligned}\nu_a(13) =& \frac{(1-d_{es}(t,loc))\underline{E}_a(13)+d_{es}(t,loc)\overline{E}_a(13)}{n}\\ =& \frac{(1-0.7)\times 4.656+0.7\times 6}{10}\\ =& 0.56.\end{aligned}$$

Similarly, we can obtain:

$$\begin{aligned}&\nu_g(13)=0.547,\\ &\nu_{\mathrm{IPL}}(13)=0.691.\end{aligned}$$

(vii) We can calculate the overall degree of potential threat of each watched object after considering all relative attributes at 9:15 pm by the weighted aggregation operator in formula (10). Suppose $\tau=0.5$, for the person p_{13} in the foreign currency exchange shop, we have

$$\begin{aligned}g(0.3,\nu_a(13)) =& w_a\nu_a(13)+(1-w_a)\tau\\ =& 0.3\times 0.56+(1-0.3)\times 0.5\\ =& 0.518.\end{aligned}$$

Similarly, we have:

$$g(0.3, \nu_g(13)) = 0.514,$$
$$g(0.8, \nu_{\text{IPL}}(13)) = 0.653.$$

Thus, by formula (9), we have

$$\begin{aligned} & R(g(0.3, \nu_a(13)), g(0.3, \nu_g(13)), g(0.8, \nu_{\text{IPL}}(13))) \\ =& \frac{1}{1 + (\frac{0.5}{1-0.5})^{3-1} \times \frac{(1-0.518)(1-0.514)(1-0.653)}{0.518 \times 0.514 \times 0.653}} \\ =& 0.681. \end{aligned}$$

Similarly, for the person p_{19} in the control centre, we can obtain

$$R(g(0.3, \nu_a(19)), g(0.3, \nu_g(19)), g(0.8, \nu_{sr}(19))) = 0.843.$$

Thus, we can rank the potential threat of the watched objects according to their overall assessment by Definition 9. That is,

$$p_{19} \succeq p_{13}.$$

Therefore, the surveillance system should suggest the security team to prevent the further action of person p_{19} in the control centre first.

7. RELATED WORK

In this section, we discuss the related work to show how our work advances the state-of-art in its research field.

7.1. Threat/risk assessment

There are lots of work on threat/risk assessment, but little deal with ambiguity in threat assessment and threat caused by a potential terrorist attack and anti-social/criminal behaviour. In the following, we compare some existing studies with our study in this paper.

Naseem, Khan, and Malik[49] propose an approach for threat assessment and weapon assignment. According to threat perception, the model uses the parametric based automatic threat assessment technique for further weapon scheduling and assignment problem. The threat they studied is in combat situation and the purpose of threat assessment is to schedule weapons to maximally kill enemy. Rather, the threat we concern is about terrorist attack and anti-social/criminal behaviours, and the purpose of our threat assessment is to rank the threat degrees of multiple objects, so that we can more efficiently allocate limited security sources to prevent terrorist attack and anti-social/criminal behaviours.

Kong et al.[31] deal with the issue of threat assessment of group target that is consisted of multi-class weapons. Assessing the threat of group target is for the optimal decision of troop deployment. More specifically, they propose a multi-attribute group decision-making method to solve the interval-valued intuitionistic fuzzy threat assessment problem of group targets without known attribute weights and decision maker's preference weights. There are some significant differences between our work and theirs. First, ours is concerned with terrorist attack and anti-social/criminal behaviours instead of weapons. Second, we handle ambiguous threat by using D-S theory of evidence, while they cope with interval-valued threat by using fuzzy set theory. Third, we use a weighted uninorm operator to aggregate threat degrees of all the attributes, while they use weighted average operator.

Zharikova and Sherstjuk[68] propose a qualitative danger and threat assessment method based on the principle of the maximal allowable limits for an intelligent disaster decision

support system. Their method employs the rough set based plausible disaster spreading model and the formal model of the territorial system. Our model in this paper is different from theirs in at least two aspects: (i) our concern is threat caused by human, while theirs is that caused by natural disasters; and (ii) the tool we use to handle uncertainty is D-S theory of evidence, while that they use is rough set theory [50].

In order to address the numerous risks associated with seaport operations, John et al. [29] develop a subjective security risk analysis method to enhance the security of seaport systems. Specifically, they employs a fuzzy analytical hierarchy process to analyse the complex structure of the system and determine the weights of security systems/measures, while utilise evidential reasoning to synthesise the risk analysis. Our work is different from them in the following two aspects: (i) the security issue in our work is caused by potential terrorist attacks and anti-social/criminal behaviours, while that in their work is caused by the complex interactions of the multiplicity of stakeholders involved in their operations in seaport; and (ii) we use D-S theory of evidence to handle uncertainty, while they use fuzzy method and evidential reasoning.

Chen, Gao, and Zhong [13] deal with the threat assessment problem for unmanned aerial vehicles in modern air combat. More specifically, they use a fuzzy grey cognitive map for threat assessment in air battlefield and validate their method. Our work in this paper is different from them in the following two aspects: (i) The purpose that we assess threat is to prevent terrorist attacks and anti-social/criminal behaviours, while theirs is for efficient operation of unmanned aerial vehicles in modern air combat; and (ii) we deal with ambiguity in the process of threat assessment by using D-S theory of evidence, while they deal with fuzziness by using fuzzy grey cognitive map.

To express the probability information existing in the hesitancy more conveniently, Song *et al.* [57] generalise the concept of probabilistic hesitant fuzzy set to interval-valued probabilistic hesitant fuzzy set (IVPHFS). Moreover, they propose some aggregation operators over IVPHFSs. Further, they discuss how to use IVPHFSs aggregation operators to deal with practical multi-criterion group decision making problems, for example, the problem of Arctic geopolitical risk evaluation. Our method also uses an aggregation operator based method of multi-criterion decision making to evaluate threat/risk, but ours differs from theirs in the following aspects: (i) we use D-S theory of evidence to deal with the ambiguous information, while they use fuzzy set theory to deal with interval-valued probabilistic hesitant fuzzy information; and (ii) what they evaluate is Arctic geopolitical risk, while what we do is the threat of terrorist attacks and anti-social behaviours.

Szwed, Skrzynski, and Chmiel [60] propose an efficient and low-cost risk assessment method to calculate risk based on fuzzy cognitive maps (FCMs) in a complex automated video surveillance system, which goal is to provide continuous protection of critical infrastructure and other facilities. In their model, FCMs are employed to model dependencies between assets and FCM based reasoning is employed to aggregate risks associated to assets. Although in our work surveillance system is involved, we employ D-S evidence theory to calculate the threat degree of each event according to uncertain information from multiple heterogeneous sources, which are different sensors, cameras and even human; while in their model there is only video. And in our model uncertainty is about sources' reliability and ambiguity about recognition of objects being watched, while in their model it is about fuzzy dependencies among assets. In addition, to assess an overall threat degree of an object being observed we use a weighted uninorm operator to fuse the conflict threat degrees regarding all the relevant attributes, while they use FCM based reasoning to aggregate risks associated to assets.

In order to avoid underestimating the results of security risk analysis and subsequent rank ordering of units, Khakzad, Reniers, and van Gelder [30] address the interactions among the security risk parameters (*e.g.*, the mutual influence between the type of threat and the target assets). Specifically, they use analytic network process (ANP) to security-based rank ordering of hazardous facilities such as chemical plants, because ANP can well deal with mutual interactions and overcome the disadvantage of the linearity of current security risk assessment methodologies. The main differences between their work and ours are as follows: (i) they deal

with interaction among risk parameters, while we suppose the attributes that cause threats are independent of each other; (ii) their work is concerned with the security of hazardous facilities such as chemical plants, while we concern the security of public; and (iii) we consider ambiguity in the process of assessing threat, but they do not.

Chi *et al.*[15] present a decision support system for crime linkage based on various, including behavioral, features of criminal cases. This system is based on feature similarity algorithms to calculate the pairwise similarities and build up a classifier to determine whether or not a case pair should belong to a criminal series. However, this model only focuses on the issue of detecting serial crimes from historical crime data and domain experts interaction. As a result, it only works as an off-line prediction method rather than a real-time threat detection method as our model does.

Zheng and Deng[69] propose an evaluation method based on fuzzy relations between the DempsterShafer belief structure. In their method, mass functions are used to model the occurrence rate of attributes in basic events. This is similar to our work in this paper, but their events are not specific to threat events like ours and they do not define the model of an event as we do. In their method, the membership degree functions of fuzzy sets to describe relations between events, from which the relations among basic events and the top event can be derived. Finally, they use Dempster combination rule, pignistic probability, and a belief measure to evaluate these relations among events. However, what we evaluate is events themselves (*i.e.*, events threat degrees according to the information from all the sources) rather the relations among them. In addition, their examples for illustrating their evaluation method is numerical (without any specific meaning), while ours is a specific scenario in an intelligent surveillance system.

7.2. Security game for crime prevention

Our work in this paper is actually on crime prevention. In the field of crime prevention, there are a lot of studies on security games. In such a game, suppose an attacker attempts to attack a number of targets, while the defender tries to protect them. However, the defender has limited resources and cannot protect all targets at the same time. Then how to allocate limited resources to best protect many targets and minimise possible losses? The researchers answered this question in various situations. For example, Ma, Luo, and Liu[43] study that when the payoffs that an attacker attacks different targets of the attacker and the defender protect the different targets are uncertain or only in a rough range and even completely unknown, how the defender chooses countermeasures. Ma *et al.*[42] also analyses the type of attacker, predicts the target of possible attacks, and the actions that may be taken, and finds the defender's strategy. Zhang, Luo, and Ma[67] studied how defenders should respond when the type of attacker is ambiguous. Zhang and Luo[66] also studied how defenders should respond when an attacker can observe partially the defender's behaviour. These are all issues related to the allocation of resources in advance. In addition, Ma *et al.*[44] also studied the allocation of real-time security resources under uncertain and ambiguous situations. All of the above studies are based on D-S theory of evidence theory and the decision-making psychology that people try to avoid the ambiguous choice and like a choice that has as low regret as possible.

All these security games assume the payoffs of defenders' choices and attackers' choices are known. In other words, they suppose the defender knows threat degrees of the attackers to different targets and then find the optimal security source allocation to prevent crimes. However, our work in this paper tries to figure out threat degrees of objects being watched.

7.3. Information fusion

The problem of information fusion has become one of key challenges in the realm of intelligent systems[35,39,64]. A common method to address this challenge is to use aggregation operators. Albusac *et al.*[5] analyse different aggregation operators and proposed a new aggregation method based on the Sugeno integral for multiple attributes in the domain of intelligent surveillance. Also, Rudas, Pap, and Fodor[53] offer a comprehensive study of information aggregation in

intelligence systems from different application fields, such as robotics, vision, knowledge based systems, and data mining. Aggarwal[2] uses the generalised attitudinal Choquet integral operator to present utility function of a decision maker and learn its parameters. And our method indeed employs a uninorm aggregation operator for information fusion in threat assessment under uncertainty.

We actually applied a uninorm aggregation operator into a specific Multi-Attribute DecisionMaking (MADM) problems. Recently there are a lot of studies to do so. For example, Garg and Arora[25] develop some new power aggregation operators for intuitionistic fuzzy soft numbers and applied these operators into MADM problems. Garg[24] identifies two new exponential operational laws about the intervalvalued Pythagorean fuzzy set, presents their corresponding aggregation operators and an MADM approach based on these operators. Ashraf and Abdullah[6] introduce the concept of spherical fuzzy sets, extend different strict archimedean triangular norm and conorm to aggregate spherical fuzzy information, and establish a group MADM method based on these operators. Jana *et al.*[27] discuss how to apply picture fuzzy Dombi aggregation operator to MADM process. However, all their decision-making problems are specific to threat assessment as ours is.

7.4. Event processing

Based on D-S theory of evidence, Calderwood *et al.*[10] present an event modelling and reasoning framework where events observed from heterogeneous sources may be uncertain or incomplete, and sensors may be unreliable or in conflict. So their work is quite similar to ours, but their framework cannot help security teams figure out which event is the most dangerous. Also, Calderwood *et al.*[9] study how to fuse the uncertain and incomplete information from heterogeneous sources which may be unreliable or conflicting. They use D-S theory of evidence to model the sensor information, but they employ a different method, called context-dependent combination, to fuse the information. They claim their fusion method has some advances over the Dempster combination rule in D-S theory of evidence. Although we do not have their advances when fusing sensor information, they did not study how to rank the fused information to figure out the most dangerous event, but we do.

Flouris *et al.*[22] survey the main research issues in existing complex event processing techniques, especially in the optimisation aspect of query on event streams. However, their event data are generated from machine-to-machine interactions and Internet-of-Things platforms, while ours are from sensors in intelligent surveillance systems. And their focus is on the optimisation aspect of query on event streams, but ours is on how to rank threat events. Finally, although they investigate probabilistic events, the ambiguous events are not involved in their work; while we use D-S theory to deal with ambiguous events.

Dayarathna and Perera[16] also provide another survey on event processing. In particular, they investigate the system architecture characteristics of novel platforms of event processing, identify significant advancements in novel application areas (*e.g.*, the Internet of Things, streaming machine learning, and processing of complex data types such as text, video data streams, and graphs), and discuss some work on event ordering, system scalability, event processing languages, and heterogeneous devices usage for event processing. However, they did not discuss the ambiguous event processing in intelligent surveillance systems, which we deal with in this paper.

Ma *et al.*[40] propose a real-time event composition framework which can infer malicious situations (composite events) from a set of correlated atomic events based on uncertain or imperfect information gathered from multiple sources. This is similar to our work in this paper, but their framework does not support decision making. Moreover, their event model is very simple. More specifically, after considering the challenges for the multi-attribute issue, our event model in this paper remains their components of event type (T_e) and source ID (ID_s), whilst put more components into consideration, including the time duration of an event (t_e), the location information of an event (loc), the ID of a watched object/person (ID_p), the reliability degree of a given source ($d_{sr}(ID_s)$), the criticality function of an event ($d_{es}(t, loc)$),

the weight function of an attribute (w_c), mass function m_c, and utility function u_c. Therefore, ours is more convenient and intuitive than the one proposed by Ma *et al.*[40]. For example, suppose a sensor captures a person sitting in the waiting area of an airport from 21:15 to 22:00. Then in our model, it should be considered as one event; but in that of Ma *et al.*[40], it needs to be viewed as a set of events, each of which has its own mass function that cannot combine together since they have different times of occurrence.

8. CONCLUSIONS

In this paper, we propose a novel framework that can help a security team to choose the dangerous event to deal with when facing ambiguous information of multiple watched object from unreliable sources in a sensors network. More specifically, we propose video-analytic and sensor measurements in the shape of multi-attribute events. Further, we introduce the rules for the inference of event with a potential threat. Then, we assess the threats of watched objects by integrating the techniques of D-S theory of evidence, generalised expected utility theory, and a weighted uninorm aggregation operator. Thus, we can rank the potential threat of multiple watched objects according to the conflicting, ambiguous information provided by multiple sensors or classification algorithms. That is, we assess the threat of each watched object according to the potential dangerous degrees of the characteristics of various watched objects as well as the threat degree of the watched object revealed by the ambiguous information in the sensor network.

There are a number of avenues for further work to follow what we did in this paper. First, it is worth discussing the differences among various decision making principle in uncertain theory for security surveillance, such as the principle of insufficient reason, minimax regret, maximin expected utility[20], and the ambiguity aversion principle of minimax regret[45]. Second, in the case of limited security resources[11] and the different importance of various surveillance environments, a security manager needs to reduce the consumption of security resources, or pay more attention to avoiding unacceptable losses. Therefore, it is necessary to construct or choose a flexible aggregation operator that can reflect individualities of different security managers in combining evidence from different sources in different surveillance environments. Some clues of such aggregation operators may be hidden in some recent work on aggregation operators in multi-criterion decision making[38,25,59]. Third, in a real-time surveillance environment, if the suspects have more than one potential attack targets but the security resources are limited, the security manger needs to consider the suspect's simultaneously response to the security coverage, the suspect's uncertain preferences, and his plan according to the information from the surveillance system. In this case, it is reasonable to employ game theory to better allocate the security resource according to the threat information available in our framework.

ACKNOWLEDGEMENTS

The work described in this paper was supported by the National Natural Science Foundation of China (Nos. 61772210, 61272066, 61806080, and 61762016), Humanities and Social Sciences Foundation of Ministry of Education of China (No. 18YJC72040002), Guangdong Province Universities and Colleges Pearl River Scholar Funded Scheme (2018), the Project of Science and Technology in Guangzhou in China (No. 201807010043), and the key project in universities in Guangdong Province of China (No. 2016KZDXM024).

REFERENCES

[1] Roy J Adams, Abhinav Parate, and Benjamin M Marlin. Hierarchical span-based conditional random fields for labeling and segmenting events in wearable sensor data

streams. In *Proceedings of the 33rd International Conference on Machine Learning*, pages 334–343, 2016.

[2] Manish Aggarwal. Learning of aggregation models in multi criteria decision making. *Knowledge-Based Systems*, 119:1– 9, 2017.

[3] Malek Al-Nawashi, Obaida M Al-Hazaimeh, and Mohamad Saraee. A novel framework for intelligent surveillance system based on abnormal human activity detection in academic environments. *Neural Computing and Applications*, 28(Suppl 1):1–8, 2016.

[4] Wathiq Laftah Al-Yaseen, Zulaiha Ali Othman, and Mohd Zakree Ahmad Nazri. Real-time multi-agent system for an adaptive intrusion detection system. *Pattern Recognition Letters*, 85:56–64, 2017.

[5] Javier Albusac, David Vallejo, Luis Jiménez, Jose Jesus Castro-Schez, and Carlos Glez-Morcillo. Combining degrees of normality analysis in intelligent surveillance systems. In *15th International Conference on Information Fusion*, pages 2436–2443, 2012.

[6] Shahzaib Ashraf and Saleem Abdullah. Spherical aggregation operators and their application in multiattribute group decision-making. *International Journal of Intelligent Systems*, 34(3):493–523, 2019.

[7] Nicola Basilico, Giuseppe De Nittis, and Nicola Gatti. Adversarial patrolling with spatially uncertain alarm signals. *Artificial Intelligence*, 246:220–257, 2017.

[8] Luca Bonini, Pier Francesco Ferrari, and Leonardo Fogassi. Neurophysiological bases underlying the organization of intentional actions and the understanding of others intention. *Consciousness and Cognition*, 22(3):1095–1104, 2013.

[9] Sarah Calderwood, Kevin McAreavey, Weiru Liu, and Jun Hong. Context-dependent combination of sensor information in dempster-shafer theory for bdi. *Knowledge and Information Systems*, 51(1):259–285, 2017.

[10] Sarah Calderwood, Kevin McAreavey, Weiru Liu, and Jun Hong. Modelling and reasoning with uncertain event-observations for event inference. In *ICAART (2)*, pages 308–317, 2017.

[11] M. Camacho-Collados and F. Liberatore. A decision support system for predictive police patrolling. *Decision Support Systems*, 75:25 – 37, 2015.

[12] E. Carrabine, P. Cox, M. Lee, N. South, K. Plummer, and J. Turton. *Criminology: A sociological introduction*. Routledge, 2009.

[13] Jun Chen, Xudong Gao, and Linhui Zhong. Using fuzzy grey cognitive maps to model threat assessment for UAVs. In *2018 IEEE 14th International Conference on Control and Automation*, pages 594–599, 2018.

[14] Fanny Chevalier, Pierre Dragicevic, and Steven Franconeri. The not-so-staggering effect of staggered animated transitions on visual tracking. *IEEE Transactions on Visualization and Computer Graphics*, 20(12):2241–2250, 2014.

[15] Hong Chi, Zhihong Lin, Huidong Jin, Baoguang Xu, and Mingliang Qi. A decision support system for detecting serial crimes. *Knowledge-Based Systems*, 123:88–101, 2017.

[16] Miyuru Dayarathna and Srinath Perera. Recent advancements in event processing. *ACM Computing Surveys (CSUR)*, 51(2):33, 2018.

[17] Paulo Vitor de Campos Souza, Gustavo Rodrigues Lacerda Silva, and Luiz Carlos Bambirra Torres. Uninorm based regularized fuzzy neural networks. In *2018 IEEE conference on evolving and adaptive intelligent systems (EAIS)*, pages 1–8. IEEE, 2018.

[18] Arthur Dempster. Upper and lower probabilities induced by a multivalued mapping. In *Classic Works of the Dempster-Shafer Theory of Belief Functions*, volume 219 of *Studies in Fuzziness and Soft Computing*, pages 57–72. Springer, 2008.

[19] Dawei Du, Longyin Wen, Honggang Qi, Qingming Huang, Qi Tian, and Siwei Lyu. Iterative graph seeking for object tracking. *IEEE Transactions on Image Processing*, 27(4):1809–1821, 2017.

[20] Johanna Etner, Meglena Jeleva, and Jean-Marc Tallon. Decision theory under ambiguity. *Journal of Economic Surveys*, 26(2):234–270, 2012.

[21] Hélène Fargier and Romain Guillaume. Sequential decision making under uncertainty: Ordinal uninorms vs. the hurwicz criterion. In *International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems*, pages 578–590. Springer, 2018.

[22] Ioannis Flouris, Nikos Giatrakos, Antonios Deligiannakis, Minos Garofalakis, Michael Kamp, and Michael Mock. Issues in complex event processing: Status and prospects in the big data era. *Journal of Systems and Software*, 127:217–236, 2017.

[23] Vittorio Gallese and Alvin Goldman. Mirror neurons and the simulation theory of mind-reading. *Trends in cognitive sciences*, 2(12):493–501, 1998.

[24] Harish Garg. New exponential operational laws and their aggregation operators for interval-valued pythagorean fuzzy multicriteria decision-making. *International Journal of Intelligent Systems*, 33(3):653–683, 2018.

[25] Harish Garg and Rishu Arora. Generalized intuitionistic fuzzy soft power aggregation operator based on t-norm and their application in multicriteria decision-making. *International Journal of Intelligent Systems*, 34(2):215–246, 2019.

[26] Xin Hong, Yan Huang, Wenjun Ma, Sriram Varadarajan, Paul Miller, Weiru Liu, Maria Jose Santofimia Romero, Jesus Martinez del Rincon, and Huiyu Zhou. Evidential event inference in transport video surveillance. *Computer Vision and Image Understanding*, 144:276–297, 2016.

[27] Chiranjibe Jana, Tapan Senapati, Madhumangal Pal, and Ronald R Yager. Picture fuzzy dombi aggregation operators: Application to madm process. *Applied Soft Computing*, 74:99–109, 2019.

[28] Xiaoxin Jing, Xudong Luo, and Youzhi Zhang. A fuzzy dynamic belief logic system. *International Journal of Intelligent Systems*, 29(7):687–711, 2014.

[29] Andrew John, Zaili Yang, Ramin Riahi, and Jin Wang. A decision support system for the assessment of seaports security under fuzzy environment. In *Modeling, Computing and Data Handling Methodologies for Maritime Transportation*, pages 145–177. Springer, 2018.

[30] Nima Khakzad, Genserik Reniers, and Pieter van Gelder. A multi-criteria decision making approach to security assessment of hazardous facilities. *Journal of Loss Prevention in the Process Industries*, 48:234–243, 2017.

[31] Depeng Kong, Tianqing Chang, Quandong Wang, Haoze Sun, and Wenjun Dai. A threat assessment method of group targets based on interval-valued intuitionistic fuzzy multi-attribute group decision-making. *Applied Soft Computing*, 67:350–369, 2018.

[32] Weiru Liu, John G Hughes, and Michael F McTear. Representing heuristic knowledge in ds theory. In *Proceedings of the Eighth International Conference on Uncertainty in Artificial Intelligence*, pages 182–190, 1992.

[33] John D Lowrance, Thomas D Garvey, and Thomas M Strat. A framework for evidential-reasoning systems. In *Classic Works of the Dempster-Shafer Theory of Belief Functions*, volume 219 of *Studies in Fuzziness and Soft Computing*, pages 419–434. Springer, 2008.

[34] Wenhan Luo, Björn Stenger, Xiaowei Zhao, and Tae-Kyun Kim. Automatic topic discovery for multi-object tracking. In *AAAI Conference on Artificial Intelligence*, pages 3820–3826, 2015.

[35] Xudong Luo and Nicholas R Jennings. A spectrum of compromise aggregation operators for multi-attribute decision making. *Artificial Intelligence*, 171(2):161–184, 2007.

[36] Xudong Luo, Nicholas R Jennings, Nigel Shadbolt, Ho-fung Leung, and Jimmy Ho-man Lee. A fuzzy constraint based model for bilateral, multi-issue negotiations in semi-competitive environments. *Artificial Intelligence*, 148(1-2):53–102, 2003.

[37] Xudong Luo, Yufeng Yang, and Ho-fung Leung. Reward and penalty functions in automated negotiation. *International Journal of Intelligent Systems*, 31(7):637–672, 2016.

[38] Xudong Luo, Qiaoting Zhong, and Ho-fung Leung. A spectrum of weighted compromise aggregation operators: A generalization of weighted uninorm operator. *Int. J. Intell. Syst.*, 30(12):1185–1226, 2015.

[39] Xudong Luo, Qiaoting Zhong, and Hofung Leung. A spectrum of weighted compromise aggregation operators: A generalization of weighted uninorm operator. *International Journal of Intelligent Systems*, 30(12):1185–1226, 2015.

[40] Jianbing Ma, Weiru Liu, Paul Miller, and Weiqi Yan. Event composition with imperfect information for bus surveillance. In *IEEE International Conference on Advanced Video and Signal Based Surveillance*, pages 382–387, 2009.

[41] Wenjun Ma, Weiru Liu, and Jun Hong. Fusion of static and temporal information for threat evaluation in sensor networks. In *Knowledge Science, Engineering and Management*, volume 9403 of *Lecture Notes in Computer Science*, pages 66–77, 2015.

[42] Wenjun Ma, Weiru Liu, Paul Miller, and Xudong Luo. A game-theoretic approach for threats detection and intervention in surveillance. In *Proceedings of the 2014 International Conference on Autonomous Agents and Multi-agent Systems*, pages 1565–1566, 2014.

[43] Wenjun Ma, Xudong Luo, and Weiru Liu. An ambiguity aversion framework of security games under ambiguities. In *Twenty-Third International Joint Conference on Artificial Intelligence*, pages 271–278, 2013.

[44] Wenjun Ma, Kevin McAreavey, Weiru Liu, and Xudong Luo. Acceptable costs of minimax regret equilibrium: A solution to security games with surveillance-driven probabilistic information. *Expert Systems with Applications*, 108:206–222, 2018.

[45] Wenjun Ma, Wei Xiong, and Xudong Luo. A model for decision making with missing, imprecise, and uncertain evaluations of multiple criteria. *International Journal of Intelligent Systems*, 28(2):152–184, 2013.

[46] Xiao Ma, Qiao Liu, Zhenyu He, Xiaofeng Zhang, and Wen-Sheng Chen. Visual tracking via exemplar regression model. *Knowledge-Based Systems*, 106:26–37, 2016.

[47] Raymond Moodley, Francisco Chiclana, Fabio Caraffini, and Jenny Carter. Application of uninorms to market basket analysis. *International Journal of Intelligent Systems*, 34(1):39–49, 2019.

[48] Ignacio Moya, Manuel Chica, Jos L. Sez-Lozano, and scar Cordn. An agent-based model for understanding the influence of the 11-m terrorist attacks on the 2004 Spanish elections. *Knowledge-Based Systems*, 123:200–216, 2017.

[49] Afshan Naseem, Shoab Ahmed Khan, and Asad Waqar Malik. A real-time man-in-loop threat evaluation and resource assignment in defense. *Journal of the Operational Research Society*, 68(6):725–738, 2017.

[50] Zdzislaw Pawlak. Rough set theory and its applications to data analysis. *Cybernetics & Systems*, 29(7):661–688, 1998.

[51] Fangling Pu, Wentao Xie, Yao Cheng, and Xin Xu. Implementation of real-time vehicle tracking in city-scale video network. *Cybernetics and Systems*, 47(4):249–260, 2016.

[52] Guifang Qiao, Guangming Song, Ying Zhang, Jun Zhang, and Jin Peng. Lifetime optimization of an indoor surveillance sensor network using adaptive energy-efficient transmission. *International Journal of Distributed Sensor Networks*, 2015:1–12, 2015.

[53] Imre J Rudas, Endre Pap, and JáNos Fodor. Information aggregation in intelligent systems: An application oriented approach. *Knowledge-Based Systems*, 38:3–13, 2013.

[54] Dinesh Satre, Akshaya Morye, Priyanvada Dhamane, Priyanka Khedkar, and Suraj Kulkarni. Motion detection and video surveillance system. *International Journal of Engineering Science*, 6(5):5441–5446, 2016.

[55] Glenn Shafer. *A mathematical theory of evidence*. Princeton University Press, Princeton, 1976.

[56] Karan Sikka, Abhinav Dhall, and Marian Bartlett. Exemplar hidden markov models for classification of facial expressions in videos. In *Proceedings of the 2015 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 18–25, 2015.

[57] Chenyang Song, Hua Zhao, Zeshui Xu, and Zhinan Hao. Interval-valued probabilistic hesitant fuzzy set and its application in the arctic geopolitical risk evaluation. *International Journal of Intelligent Systems*, 34(4):627–651, 2019.

[58] Thomas M Strat. Decision analysis using belief functions. *International Journal of Approximate Reasoning*, 4(5):391–417, 1990.

[59] Guidong Sun, Xin Guan, Xiao Yi, and Jing Zhao. Belief intervals aggregation. *International Journal of Intelligent Systems*, 33(12):2425–2447, 2018.

[60] Piotr Szwed, Pawel Skrzynski, and Wojciech Chmiel. Risk assessment for a video surveillance system based on fuzzy cognitive maps. *Multimedia Tools and Applications*, 75(17):10667–10690, 2016.

[61] Burak Uzkent, Matthew J Hoffman, and Anthony Vodacek. Real-time vehicle tracking in aerial video using hyperspectral features. In *Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 36–44, 2016.

[62] Jeffery T. Walker and Sean Maddan. *Understanding Statistics for the Social Sciences, Criminal Justice, and Criminology*. Jones & Bartlett Publishers, 2013.

[63] Ronald R Yager and Alexander Rybalov. Uninorm aggregation operators. *Fuzzy sets and Systems*, 80(1):111–120, 1996.

[64] Anis Yazidi and Enrique Herrera-Viedma. A new methodology for identifying unreliable sensors in data fusion. *Knowledge-Based Systems*, 136:85 – 96, 2017.

[65] Hasan. U. Zaman, Tarafder Elmi Tabassum, Tanha Islam, and Nadia Mohammad. Low cost multi-level home security system for developing countries. In *International Conference on Intelligent Computing and Control Systems*, pages 549–554, 2018.

[66] Youzhi Zhang and Xudong Luo. Security games with partial surveillance. In *Proceedings of the 2014 International Conference on Autonomous Agents and Multi-agent Systems*, pages 1527–1528, 2014.

[67] Youzhi Zhang, Xudong Luo, and Wenjun Ma. Security games with ambiguous information about attacker types. In *AI 2013: Advances in Artificial Intelligence*, volume 8272 of *Lecture Notes in Computer Science*, pages 14–25, 2013.

[68] Maryna Zharikova and Volodymyr Sherstjuk. Threat assessment method for intelligent disaster decision support system. In *Advances in Intelligent Systems and Computing*, volume 512 of *Advances in Intelligent Systems and Computing*, pages 81–99. Springer, 2017.

[69] Haoyang Zheng and Yong Deng. Evaluation method based on fuzzy relations between dempster–shafer belief structure. *International Journal of Intelligent Systems*, 33(7):1343–1363, 2018.

[70] Yonghua Zhou, Xin Tao, Lei Luan, and Zhihui Wang. Safety justification of train movement dynamic processes using evidence theory and reference models. *Knowledge-Based Systems*, 139:78 – 88, 2018.